EXHIBIT 1

The investigation into this incident is ongoing, and this notice will be supplemented with any substantive information learned after submission of this notice. By providing this notice, CareMeridian, LLC ("CareMeridian") does not waive any rights or defenses regarding the applicability of California law, the applicability of the California data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around December 23, 2017, CareMeridian discovered that an unencrypted disk sent to them by their third-party software provider (Bullpen Financial, Inc.) containing documents that included sensitive information appeared to have been lost in the mail. An investigation was immediately launched that included the retention of a forensics expert, to determine the nature and scope of this incident, the types of information involved and the individuals who may be affected. It was determined on January 20, 2018 that protected personal information was contained on the disk. There was information related to various entities such as CareMeridian that the third-party was auditing, so further internal investigation was required to determine individual addresses and the entity with which the impacted individuals had a relationship. This research was finalized March 12, 2018.

Notice to California Residents

While the investigation is ongoing, after review of the files believed to be stored on the disk with the assistance of an outside forensics expert, it was confirmed that the name and medical information relating to nine hundred fifty-three (953) California residents and the name and Social Security number of thirteen (13) California residents may have been accessible on the lost disk. Written notice of this incident is being provided to those impacted California residents on or about March 20, 2018, in substantially the same form as the letters attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

CareMeridian is providing the thirteen (13) individuals who potentially had their Social Security number exposed access to twelve (12) months of complimentary credit monitoring and identity restoration services with Experian. A dedicated number has been established for all impacted individuals to contact with questions or concerns regarding this incident. Additionally, CareMeridian is providing all impacted individuals with helpful information on how to protect against identity theft and fraud, including how to place a fraud alert and security freeze on one's credit file, the contact information for the national consumer reporting agencies, how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

CareMeridian is also providing notice of this incident to other state regulators as required. On January 16, 2018, CareMeridian notified the California Department [insert full name] on a preliminary basis as our investigation was still incomplete. CareMeridian is providing supplementary notice to the California Department of Public Health.

Mullen.law

EXHIBIT A

CareMeridian
313 Congress Street
5th Floor
Boston, MA 02210

March 20, 2018

[Name]
[Address]
[City, State Zip]

RE: Notice of Data Breach

Dear [Name],

[Legal Entity] is writing to notify you of a recent incident that may affect the security of personal information concerning [Individual Served Name]. Although we are unaware of any actual or attempted misuse of this information, we are providing you with information regarding the incident and steps we have taken since discovering it, as well as steps you can take to protect your personal information should you feel it is appropriate to do so.

What Happened? On December 21, 2017, [entity] discovered that an unencrypted disk sent by a third-party software provider containing documents that included sensitive information appeared to have been lost in the mail. [entity] immediately launched an investigation to determine the nature and scope of this incident, the types of information involved and the individuals who may be affected. We retained a third-party expert to assist us with these ongoing investigations. We continue to have no evidence of actual or attempted misuse of information as a result of this incident.

What Information Was Involved? While the investigations are on-going, the lost disk is believed to contain certain patient billing information including their [data elements]. Although the investigation is ongoing, Social Security number, driver's license number or any financial account information **were not compromised**.

What Are We Doing? At [entity], the confidentiality, privacy, and security of information in our care is one of our highest priorities. We have security measures in place to protect data in our care and we are taking steps to enhance data security protections to protect against similar incidents in the future. We ceased doing business with the third-party software provider. We will also be notifying the U.S. Department of Health and Human Services and any required state agency about this incident.

What You Can Do. Please review the enclosed "Privacy Safeguards" to learn more about ways to protect personal information.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 1-888-818-8990 and your call will be returned.

[Entity] sincerely apologizes for any inconvenience or concern this incident may cause.

Sincerely,

Bruce Nardella

Bruce Nardella
Chief Executive Officer

PRIVACY SAFEGUARDS

Monitor Your Accounts.

Credit Reports & Explanation of Benefits. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/

Additional Information. You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of ___ Rhode Island resident(s) may be impacted by this incident. **For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. You have the right to file a police report if they ever experience identity theft or fraud, and instances of known or suspected identity theft should be reported to law enforcement. Please note that in order to file a police report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. This notice has not been delayed by law enforcement.

CareMeridian
313 Congress Street
5th Floor
Boston, MA 02210

March 20, 2018

[Name]
[Address]
[City, State Zip]

RE: Notice of Data Breach

Dear [Name],

[Entity] is writing to notify you of a recent incident that may affect the security of personal information concerning [Individual Served Name]. Although we are unaware of any actual or attempted misuse of this information, we are providing you with information regarding the incident and steps we have taken since discovering it, as well as steps you can take to protect your personal information should you feel it is appropriate to do so.

What Happened? On December 21, 2017, [Entity] discovered that an unencrypted disk sent by a third-party software provider containing documents that included sensitive information appeared to have been lost in the mail. [Entity] immediately launched an investigation, retaining a forensics expert, to determine the nature and scope of this incident, the types of information involved and the individuals who may be affected. It was determined on January 20, 2018 that certain personal information was contained on the disk. We continue to have no evidence of actual or attempted misuse of information as a result of this incident.

***What Information Was Involved*?** While the investigations are on-going, the lost disk is believed to contain certain personal information including [data elements]. We currently have no evidence that your information was accessed or misused; however, we wanted to notify you out of an abundance of caution.

What Are We Doing? At [Entity], the confidentiality, privacy, and security of information in our care is one of our highest priorities. We have security measures in place to protect data in our care and we are taking steps to enhance data security protections to protect against similar incidents in the future. We ceased doing business with the third-party software provider. We will also be notifying the U.S. Department of Health and Human Services and any state required state agency about this incident.

Although we are unaware of any actual or attempted misuse of the information, as an added precaution, we arranged to have Experian protect [Individual Served Name] identity for one (1) year at no cost to you. Please review the instructions contained in the attached Privacy Safeguards to enroll and receive these services. The cost of this service will be paid for by

[Entity]. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll [Individual Served Name] in the credit monitoring service.

What You Can Do. Please review the enclosed "Privacy Safeguards" to learn more about ways to protect personal information.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 1-888-818-8990 and your call will be returned.

[Entity] sincerely apologizes for any inconvenience or concern this incident may cause.

Sincerely,

Bruce Nardella

Bruce Nardella
Chief Executive Officer

PRIVACY SAFEGUARDS

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one (1) year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary one (1) year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: June 30, 2018 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: [code]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by June 30, 2018. Be prepared to provide engagement number [engagement number] as proof of eligibility for the identity restoration services by Experian.

Monitor Your Accounts.

Credit Reports & Explanation of Benefits. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/

Additional Information. You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of two (2) Rhode Island resident(s) may be impacted by this incident. This notice has not been delayed by law enforcement.